日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　８月　３日

出願番号
Application Number: 特願２０００－２３５６０５

出願人
Applicant(s): ソニー株式会社

２００１年　５月３０日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０４４７５５

【書類名】　特許願

【整理番号】　0000540801

【提出日】　平成12年 8月 3日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/177

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　末吉　正弘

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【連絡先】　知的財産部　０３－５４４８－２１３７

【手数料の表示】

【予納台帳番号】　005094

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　ＯＳ上のセキュアなタスク間通信方法

【特許請求の範囲】

【請求項１】　ＯＳ（オペレーティング・システム）上で実行されるタスク自身の鍵からタスクと上記ＯＳとの相互認証が成功したセキュリティ有りのレベルと相互認証を行っていないセキュリティ無しのレベルとに分類して、各タスク自身のセキュリティの有無とタスクと上記ＯＳとの相互認証用鍵とを上記ＯＳ側でテーブル形式で管理する第１ステップと、

上記ＯＳ側で管理されている上記セキュリティ有りのレベルのタスクのブロックごとと、上記セキュリティ無しのレベルのタスクのブロックごとにセキュア・メモリ管理機構によりセキュア・メモリ・ブロックと、ノン・セキュア・メモリ・ブロックに分けて読み書きする第２ステップと、

上記セキュリティ有りのレベルのタスクのメイル送信用タスク上にメイル送信用バッファを用意するとととともに、上記セキュリティ有りのレベルのタスクのメイル受信用タスク上にメイル受信用バッファを用意して、上記ＯＳ内にメイル内容を格納するメモリ領域と管理情報を格納するメモリ領域とを用意する第３ステップと、

上記メイル送信用タスクでセキュリティ・レベル以外にメイルＩＤ、送信タスク側で割り当てられたメイル本体へのアドレスを指定し、ＯＳ側で上記メイル送信用タスクのセキュリティ・レベルと送信用関数のセキュリティ・レベルを基にどのメモリ・ブロックを使用するかを判断して、メイル送信用タスクがセキュリティ有りで、かつ送信時レベルがセキュリティ有りの場合のみ、上記セキュリティ・メモリ・ブロックに管理情報を書き込み、メイル送信内容をメイルＩＤ、管理情報のアドレス値、メイル本体のアドレス値を鍵として暗号化した内容を書き込む第４ステップと、

上記メイル受信用タスク側で、セキュリティ・レベル以外に上記メイル送信用タスクと同一のメイルＩＤ、メイル受信用タスク側で割り当てられたメイル本体へのアドレスを指定し、上記ＯＳによりメイル受信用タスクのセキュリティ・レベルと受信関数のセキュリティ・レベルを基にどのセキュリティ・メモリ・ブロ

ックを使用するかを判断して、メイル受信用タスクがセキュリティ有りであり、かつ受信時レベルがセキュリティ有りの場合のみ、上記セキュリティ・メモリ・ブロックで管理されているメイル受信用タスク宛ての該当受信メイルを検索して、受信内容が存在するバッファの内容をメイルＩＤ、管理情報のアドレス値、メイル本体のアドレス値を鍵として復号化した内容を上記メイル受信用タスク上のバッファにコピーする第５ステップと、

を含むことを特徴とするＯＳ上のセキュアなタスク間通信方法。

【請求項２】　上記認証は、タスクごとに持つ鍵を上記セキュアＯＳ側で管理している鍵と同一であるか、否かの照合により行うことを特徴とする請求項１記載のＯＳ上のセキュアなタスク間通信方法。

【請求項３】　上記セキュア・メモリ管理機構は、上記メモリ・ブロックをブロックごとにセキュリティ・レベルに応じたアクセス許可、不許可の設定が可能なハードウェアであることを特徴とする請求項１記載のＯＳ上のセキュアなタスク間通信方法。

【請求項４】　上記セキュア・メモリ管理機構は、セキュリティ・レベル無しのメイル送信用タスクあるいはメイル受信用タスクに対してセキュリティ有りのメモリ・ブロックへの読み書きはできないことを特徴とする請求項１記載のＯＳ上のセキュアなタスク間通信方法。

【請求項５】　上記セキュアＯＳは、タスクごとのセキュリティ・レベルの管理と上記セキュア・メモリ管理機構を介した上記メモリ・ブロックの管理を一元的に行うことを特徴とする請求項１記載のＯＳ上のセキュアなタスク間通信方法。

【請求項６】　上記管理情報は、メイル・サイズとメイル本体のポインタとで構成されることを特徴とする請求項１記載のＯＳ上のセキュアなタスク間通信方法。

【請求項７】　上記メイル送信用タスクの内容は、実態を上記セキュア・メモリ・ブロック中に有るセキュア・メモリ・プールから確保することを特徴とする請求項１記載のＯＳ上のセキュアなタスク間通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、ＯＳとＯＳ上で実行されるタスクの構成において、タスク自身のセキュリティ・レベルと、タスク側で送信、受信時に指定されるセキュリティ用モードの有無をＯＳ側で判定し、セキュリティ有りの場合はアクセス制限されたメモリ領域から通信用作業領域を獲得し、送信内容を暗号化するようにしたＯＳ上のセキュアなタスク間通信方法に関する。

【０００２】

【従来の技術】

通常のＯＳ上のタスク間通信においては、送受信されるデータ内容を隠蔽および秘匿するための記憶が存在しないために、第三者が制作したソフトウェア・モジュールにより読み書きすることが可能である。

そこで、ＯＳを介して伝送されるデータの隠蔽を実現するため、送信側タスクが設定するセキュリティの有無に応じたタスク間通信（たとえば、メイル）を実現可能な機構を発明するに至った。

たとえば、特開平０８－１０６４４１号公報では、マイクロアーキテクチャ方式のＯＳを前提としてセキュリティ・レベルを持つプロセス間通信方式が記載されている。

【０００３】

【発明が解決しようとする課題】

しかし、この公報の場合には、ＯＳ外部に認証局に相当するトラスティド・サーバが必要であるという課題がある。

【０００４】

この発明は、上記従来の課題を解決するためになされたもので、認証局をＯＳの外に持たない代わりに、ＯＳ自身が送信内容本体のハードウェアによるアクセス制限と送信内容の暗号化を実現することにより、組み込み用途に配慮することができ、セキュリティ・レベルに応じたタスク処理が混在した環境で、鍵操作や暗号化、復号化を行うタスクにはセキュリティ有りのレベルを与え、セキュリティをもつタスク間通信の秘匿性を高めることができ、タスクとタスク間通信のサ

ービス起動時にセキュリティ・レベルが個別に指定可能であり、両者の組み合せによりタスク間通信の内容本体のアクセス制限が実現できるＯＳ上のセキュアなタスク間通信方法を提供することを目的とする。

【０００５】

【課題を解決するための手段】

上記目的を達成するために、この発明のＯＳ上のセキュアなタスク間通信方法は、ＯＳ（オペレーティングシステム）上で実行されるタスク自身の鍵からタスクと上記ＯＳとの相互認証が成功したセキュリティ有りのレベルと相互認証を行っていないセキュリティ無しのレベルとに分類して、各タスク自身のセキュリティの有無とタスクと上記ＯＳとの相互認証用鍵とを上記ＯＳ側でテーブル形式で管理する第１ステップと、上記ＯＳ側で管理されている上記セキュリティ有りのレベルのタスクのブロックごとと、上記セキュリティ無しのレベルのタスクのブロックごとにセキュア・メモリ管理機構によりセキュア・メモリ・ブロックと、ノン・セキュア・メモリ・ブロックに分けて読み書きする第２ステップと、上記セキュリティ有りのレベルのタスクのメイル送信用タスク上にメイル送信用バッファを用意するととともに、上記セキュリティ有りのレベルのタスクのメイル受信用タスク上にメイル受信用バッファを用意して、上記ＯＳ内にメイル内容を格納するメモリ領域と管理情報を格納するメモリ領域とを用意する第３ステップと、上記メイル送信用タスクでセキュリティ・レベル以外にメイルＩＤ、送信タスク側で割り当てられたメイル本体へのアドレスを指定し、ＯＳ側で上記メイル送信用タスクのセキュリティ・レベルと送信用関数のセキュリティ・レベルを基にどのメモリブロックを使用するかを判断して、メイル送信用タスクがセキュリティ有りで、かつ送信時レベルがセキュリティ有りの場合のみ、上記セキュリティ・メモリ・ブロックに管理情報を書き込み、メイル送信内容をメイルＩＤ、管理情報のアドレス値、メイル本体のアドレス値を鍵として暗号化した内容を書き込む第４ステップと、上記メイル受信用タスク側で、セキュリティ・レベル以外に上記メイル送信用タスクと同一のメイルＩＤ、メイル受信用タスク側で割り当てられたメイル本体へのアドレスを指定し、上記ＯＳによりメイル受信用タスクのセキュリティ・レベルと受信関数のセキュリティ・レベルを基にどのセキュリテ

ィ・メモリ・ブロックを使用するかを判断して、メイル受信用タスクがセキュリティ有りであり、かつ受信時レベルがセキュリティ有りの場合のみ、上記セキュリティメモリ・ブロックで管理されているメイル受信用タスク宛ての該当受信メイルを検索して、受信内容が存在するバッファの内容をメイルＩＤ、管理情報のアドレス値、メイル本体のアドレス値を鍵として復号化した内容を上記メイル受信用タスク上のバッファにコピーする第５ステップとを含むことを特徴とする。

そのため、メイル送信用タスクと、メイル受信用タスク自身のセキュリティ・レベルと、タスク側で送信時、受信時に指定するセキュリティ用モード有りとセキュアＯＳ側で判断すると、セキュアＯＳ側が転送用データの実態とタスク間通信路を確立するための管理用データをセキュア・メモリ・ブロックに割り当て、セキュアＯＳ側で転送用データを鍵により暗号化し、メイル受信用タスクのデータを復号化する。

また、タスクとタスク間通信のサービス起動時にセキュリティ・レベルが個別に指定可能となる。

【０００６】

【発明の実施の形態】

次に、この発明によるＯＳ上のセキュアなタスク間通信方法の実施の形態について図面に基づき説明する。

具体的な実施の形態の説明に先立ち、まず、この発明の特徴を概説する。この発明は、ＯＳとＯＳ上で実行されるタスクの構成において、タスク自身のセキュリティ・レベルとタスク側で送信、受信時に指定するセキュリティ用モードの有無をＯＳ側で判断し、セキュリティ・レベルの異なるタスク間通信路を実現する。

また、セキュリティ用モードが有りと判断された場合には、ＯＳが転送用データの実態およびタスク間通信路を確立するための管理用データをアクセス制限されたメモリに割り当てる。

一方、セキュリティ用モードが無いと判断された場合には、両者のデータをアクセス制限の無い一般のメモリに割り当てる。

さらに、タスク側でセキュリティ用モードが有りと判断された場合には、ＯＳ

が転送用データの実態を鍵により暗号化する。

【０００７】

次に、このような特徴を有するこの発明による第１実施の形態を詳細に説明する。

説明の都合上、図２から説明する。

この図２は、この第１実施の形態に適用されるセキュアＯＳ１上のタスク２、３のセキュリティ・レベルを説明するための説明図である。

この第１実施の形態では、セキュリティ有り、無しの２つのレベルを想定している。

セキュアＯＳ１側とタスクとによる相互認証が成功したタスク２、３（図２では、タスク２をタスクＡ,タスクＢとして示している。）をセキュリティ有りのレベルとし、また、この相互認証を行っていないか、相互認証の失敗、または未処理のタスク３（図２では、タスクCとして示している）をセキュリティ無しのレベルとする。

【０００８】

このセキュアＯＳ１側とタスク２，３とによる相互認証の方法は、たとえば、タスク２，３ごとに鍵を持ち、セキュアＯＳ１側で管理している鍵とタスク２，３の持っている鍵とが一致した場合にセキュリティ有りのレベルとし、また、両者の鍵が一致しない場合には、セキュリティ無しのレベルとし、図２では、上述のように、タスク３がセキュリティ無しのレベルとしている場合を示している。

これらのタスク２，３自身のセキュリティの有無と相互認識用鍵をセキュアＯＳ１側がテーブル４の形式で管理する。

すなわち、セキュリティ有りのレベルのタスク２、セキュリティ無しのレベルのタスク３、これらのタスク２、３の持っている鍵の各データはこのテーブル４の形式でセキュアＯＳ１側の内部で保持している。

【０００９】

次に、セキュアＯＳ１側のメモリ・ブロック管理について図１を参照して説明する。この図１における読み書き可能なＲＡＭなどによるメモリ・ブロック５は、ノン・セキュア・メモリ・ブロック５ａと、セキュア・メモリ・ブロック５ｂ

とに２分されている。

ノン・セキュア・メモリ・ブロック５ａには、ＮＯ．１、３、……，ｎ－１のように奇数番目のアドレスにタスク３のようなセキュリティ無しのレベルがブロックで書き込まれる。

また、セキュア・メモリ・ブロック５ｂには、ＮＯ．２，４，……、ｎのように偶数番目のアドレスにタスク２のようなセキュリティ有りのレベルがブロックで書き込まれる。

〔００１０〕

すなわち、メモリ・ブロック５は、タスクをブロックごとにセキュリティ・レベルの設定が可能なＭＭＵ６（メモリ管理機構：以下、ＳＭＭＵという）により読み書きする。

このＳＭＭＵ６は、読み書きする側のセキュリティ・レベル、すなわち、セキュアＯＳ１側のセキュリティ・レベル（さらに換言すれば、サービスを要求したタスクのセキュリティ・レベル）とノン・セキュア・メモリ・ブロック５ａに書き込まれているセキュリティ・レベルと、セキュア・メモリ・ブロック５ｂに書き込まれているセキュリティ・レベルとをを比較して、読み書きする側のセキュリティ・レベルが低い場合には、セキュリティ・アクセス違反例外が発生し、セキュア・メモリ・ブロック５ｂ、ノン・セキュア・メモリ・ブロック５ａへ読み書きが不可能になる。

〔００１１〕

言い換えれば、サービスを要求したタスクよりも、セキュリティ・レベルが高いセキュア・メモリ・ブロック５ｂ、ノン・セキュア・メモリ・ブロック５ａへのアクセスがセキュリティ・アクセス違反例外が発生してセキュア・メモリ・ブロック５ｂ、ノン・セキュア・メモリ・ブロック５ａへ読み書きが不可能になる。

このＳＭＭＵ６は、メモリ５をセキュア・メモリ・ブロック５ｂ、ノン・セキュア・メモリ・ブロック５ａごとに、セキュリティ・レベルに応じたアクセス許可、不許可の設定が可能なハードウェアである。

たとえば、このＳＭＭＵ６は、セキュリティ・レベル無しの状態で、セキュリ

ティ有りのセキュア・メモリ・ブロック５ｂへの読み書きはできないものとする。

【００１２】

セキュア・メモリ・ブロック５ｂ、ノン・セキュア・メモリ・ブロック５ａに対するセキュリティ・レベルの設定は、セキュアＯＳ１の初期時にＳＭＭＵ６により、テーブル７に示すように行う。

このテーブル７は、セキュア・メモリ・ブロック５ｂ、ノン・セキュア・メモリ・ブロック５ａのアドレスに対するセキュリティ有無と、鍵の各データが対応している。

また、セキュアＯＳ１がタスクごとのセキュリティ・レベルの管理と、ＳＭＭＵ６を介したセキュア・メモリ・ブロック５ｂ、ノン・セキュア・メモリ・ブロック５ａの管理を一元的に行う。

【００１３】

次に、セキュリティ有りタスク間通信を行う場合について図１を参照して説明する。このタスク間通信はメイルであり、上記タスク２について、図１では、メイル送信用タスク２として説明する。また、タスク３について、図１では、メイル受信用タスク３として説明する。

メイル送信用タスク２上にメイル送信用バッファ８（サーバ用バッファ）を用意するとともに、メイル受信用タスク３上にメイル受信用バッファ９を用意する。

【００１４】

また、セキュアＯＳ１内にメイル内容を格納するメモリ領域をセキュア・メモリプール１０ａ，１０ｂの形式で用意する。

管理情報を格納するメモリ領域（上記ノン・セキュア・メモリ・ブロック５ａ、セキュア・メモリ・ブロック５ｂに相当）をノン・セキュア・メモリ・キュー・リスト１１ａ、セキュア・メモリ・キュー・リスト１１ｂの形式で用意する。

図４は管理情報１２の構成を示すものであり、管理情報１２は、メイル・サイズ１２ａとメイル本体へのポインタ１２ｂで構成されている。

【００１５】

ノン・セキュア・メモリ・キュー・リスト１１ａ、セキュア・メモリ・キュー・リスト１１ｂと、セキュア・メモリ・プール１０ａ，１０ｂは、上記セキュア・メモリ・ブロック５ｂ、ノン・セキュア・メモリ・ブロック５ａに個別に用意される。

〔００１６〕

次に、メイル送信用タスク２と受信用タスク３はセキュアＯＳ1側と相互認証が正常に終了し、これらのメイル送信用タスク２と受信用タスク３自身のセキュリティ・レベルが有りに設定されている場合に、メイル送信用タスク２でタスク間通信用関数（たとえば、メイル）をセキュリティ・レベル有り付きで送信する場合の処理の流れを図５のフローチャートに沿って説明する。

まず、スタートして、メイル送信用タスク２側では、セキュリティ・レベル以外に、メイルＩＤ、メイル送信用タスク側で割り当てられたメイル本体へのアドレスを指定する。

メイル送信用タスク２がセキュリティ・オン・レベルでメイル送信サービスを要求し（ステップＳ１）、メイル送信用タスク２が送信されて、セキュアＯＳ1側でこのメイル送信用タスク２の要求を受け取ると（サービスでもよい）（ステップＳ２）、セキュアＯＳ1側では、受信したメイル送信用タスク２がセキュリティ・レベルとメイル・サービスであるかをチェックする（ステップＳ３）。

〔００１７〕

次いで、セキュアＯＳ１側では、この受信されたメイル送信用タスク２とメイル・サービスがセキュリティ・レベルであるか、どうかを判断して、さらに、送信用関数〔図８（ａ）にメイル送信関数として示されている〕のセキュリティ・レベルを基に受信されたメイル送信用タスク２に対して、セキュア・メモリ・ブロック５ｂ、あるいはノン・セキュア・メモリ・ブロック５ａのどちらのメモリブロックを使用するかを判断する（ステップＳ４）。

この判断の結果、この受信されたメイル送信用タスク２がセキュリティ有りのレベルで、かつ送信時のレベルがセキュリティ有りの場合にのみ、ステップＳ５の処理に進み、セキュアＯＳ１側では、ＳＭＭＵ６によりセキュア・メモリ・ブロック５ｂで管理されているセキュア・メモリ・キュー・リスト１１ｂの中の管

理情報とメイル本体を検索する。

【００１８】

次いで、この検索した管理情報とメイル本体から１要素のメイル本体に管理情報を書き込む。

この場合、メイル送信用タスク２の内容は、セキュリティ有りのセキュア・メモリ・ブロック５ｂに格納されているセキュア・メモリ・プール１０ｂから確保する。

次に、図６に示すメイル本体の暗号化フローチャートに示すように、セキュア・メモリ・プール１０ｂから確保したメイル送信内容のメイル本体に、ＳＭＭＵ６によりメイルＩＤを書き込み（ステップＳ１１）、管理情報のアドレス値を書き込み（ステップＳ１２）、メイル本体のアドレス値を書き込んで、これらの値を鍵としてメイル送信内容を暗号化し（ステップＳ１３）、その暗号化したメイル送信内容を、図５のステップＳ６で上記バッファ８（サーバ用バッファ）からせキュア・メモリ・キュー・リスト１１ｂで管理されるバッファ１３へコピーする。

次いで、セキュアＯＳ１側では、管理情報を更新して（ステップＳ７）、上記一連のメイル送信処理を終了する。

【００１９】

また、上記ステップＳ４の処理において、セキュアＯＳ１側では、受信されたメイル送信用タスク２のサービスのセキュリティと、さらに、タスク間通信用関数のセキュリティ・レベルを基に受信されたメイル送信用タスク２に対して、セキュア・メモリ・ブロック５ｂ、あるいはノン・セキュア・メモリ・ブロック５ａのどちらのメモリブロックを使用するかを判断した結果、受信されたメイル送信用タスク２がセキュリティ有りのレベルで、かつ送信時のレベルがセキュリティ有りでない場合には、セキュアＯＳ１側では、ＳＭＭＵ６によりノン・セキュア・メモリ・ブロック５ａから管理情報とメイル本体を検索する（ステップＳ８）。

【００２０】

次いで、セキュアＯＳ１側は、メイル本体にメイル送信用タスク２の内容を書

き込み、バッファ８に書き込んで（ステップＳ９）、上記ステップＳ７の処理を行う。

【００２１】

次に、メイル受信用タスク３でタスク間通信用関数（たとえば、メイル）をセキュリティ・レベル有り付で受信する処理の流れについて図７のフローチャートに沿って説明する。

メイル受信用タスク３側では、セキュリティ・レベル以外に、メイルＩＤ、メイル受信用タスク３側で割り当てられたメイル本体へのアドレスを指定する。メイルＩＤは、送信側と同一の値を指定する。

次いで、メイル受信用タスク３は、セキュリティ・オン・レベルのメイル受信サービスを要求し（ステップＳ２１）、メイル受信用タスク３側でメイル受信用タスク３のメイル・サービスを行うと、セキュアＯＳ１側はメイル受信用タスク３のサービスを受信する（ステップＳ２２）。

【００２２】

次いで、セキュアＯＳ１側はこの受信したメイル受信用タスク３とメイル・サービスが、セキュリティ有りのレベルであるか、否かのテェックを行い（ステップＳ２３）、そのチェックの結果、セキュリティ有りのレベルであると、次に、セキュアＯＳ１側はメイル受信用タスク３とサービスがともに、セキュリティ有りのレベルであるか、否かの判定を行い（ステップＳ２４）、その判定の結果、両方ともにセキュリティ有りのレベルであると判断すると、セキュアＯＳ１側はメイル受信用タスク３のセキュリティ・レベルと、受信用関数｛図８（ｂ）にメイル受信関数として示されている｝のセキュリティ・レベルとを基にどのセキュア・メモリ・ブロックを使用するかの判断を行う。

【００２３】

この判断の結果、メイル受信用タスク３がセキュリティ有りのレベルで、かつ受信時のレベルがセキュリティ有りのレベルの場合にのみ、セキュア・メモリ・ブロック５ｂで管理されているメイル・キュー・リスト内でのメイル受信用タスク３宛ての該当メイルを検索し（ステップＳ２５）、受信内容が存在するバッファを見付ける。

このバッファ内容をメイルＩＤ、管理情報のアドレス値、メイル本体アドレス値を鍵として復号化した内容をメイル受信用タスク３上のバッファ９へコピーする（ステップＳ２６）。

次いで、セキュアＯＳ１側は、メイル本体と管理情報とを戻して（ステップＳ２７）、一連の受信処理を終了する。

【００２４】

また、上記ステップＳ２４の処理において、セキュアＯＳ１側はメイル受信用タスク３とサービスがともに、セキュリティ・レベルであるか、否かの判定を行い（ステップＳ２４）、その判定の結果がともに、セキュリティ・レベルでない場合であると、判断すれば、セキュアＯＳ１側はノン・セキュア・メモリ・ブロック５ａにおける管理情報を検索する（ステップＳ２８）。

次いで、セキュアＯＳ１側は、メイル受信用タスク３上に用意したバッファ９にメイル本体をコピーした後に（ステップＳ２９）、上記ステップＳ２７の処理をを行う。

【００２５】

【発明の効果】

以上のように、この発明によれば、メイル送信用タスクと、メイル受信用タスク自身のセキュリティ・レベルと、タスク側で送信時、受信時に指定するセキュリティ用モード有りとセキュアＯＳ側で判断すると、セキュアＯＳ側が転送用データの実態とタスク間通信路を確立するための管理用データをセキュア・メモリ・ブロックに割り当て、セキュアＯＳ側で転送用データを鍵により暗号化し、メイル受信用タスクのデータを復号化するようにしたので、鍵操作や暗号化・復号化を行うタスクには、セキュリティ有りのレベルを与えるような、セキュリティ・レベルに応じたタスク処理が混在した環境で、タスク間通信の内容がアクセス制限される機構において、セキュリティを持つタスク間通信の秘匿性を高めることができる。

また、タスクとタスク間通信のサービス起動時にセキュリティ・レベルが個別に指定可能であり、指定されたセキュリティ・レベル２つを組み合せることによりタスク間通信の内容本体のアクセス制限を実現することができる。

【図面の簡単な説明】

【図１】

この発明によるＯＳ上のセキュアなタスク間通信方法の第１実施の形態に適用されるタスク間通信を行う場合の構成要素の説明図である。

【図２】

この発明によるＯＳ上のセキュアなタスク間通信方法の第１実施の形態に適用されるセキュアＯＳ上のタスク・セキュリティ・レベルを説明するための説明図である。

【図３】

この発明によるＯＳ上のセキュアなタスク間通信方法の第１実施の形態に適用されるセキュアＯＳ側のセキュア・メモリ・ブロックの管理を説明するための説明図である。

【図４】

この発明によるＯＳ上のセキュアなタスク間通信方法の第１実施の形態に適用されるメイル管理情報の構成説明図である。

【図５】

この発明によるＯＳ上のセキュアなタスク間通信方法の第１実施の形態に適用されるメイル送信処理を説明するためのフローチャートである。

【図６】

この発明によるＯＳ上のセキュアなタスク間通信方法の第１実施の形態に適用されるメイル本体の暗号化フローを示すフローチャートである。

【図７】

この発明によるＯＳ上のセキュアなタスク間通信方法の第１実施の形態に適用されるメイル受信処理フローを示すフローチャートである。

【図８】

この発明によるＯＳ上のセキュアなタスク間通信方法の第１実施の形態に適用されるメイル送受信関数例を示すフローチャートである。

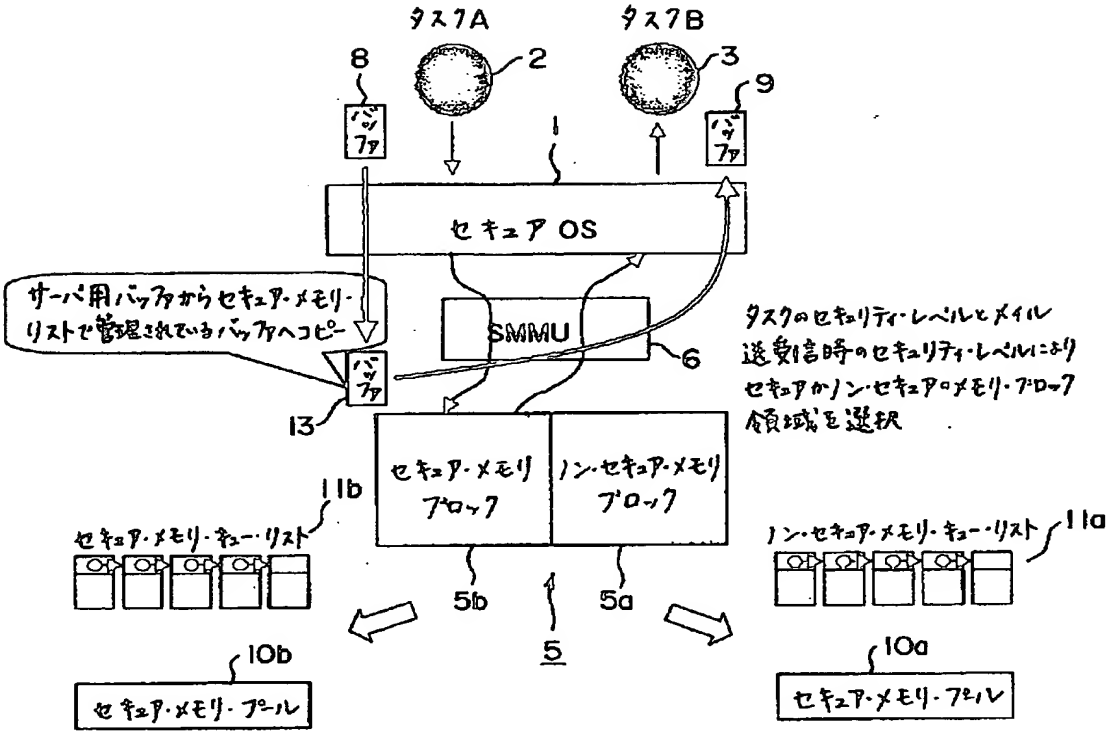
【符号の説明】

１……セキュアＯＳ，２……メイル送信用タスク、３……メイル受信用タスク

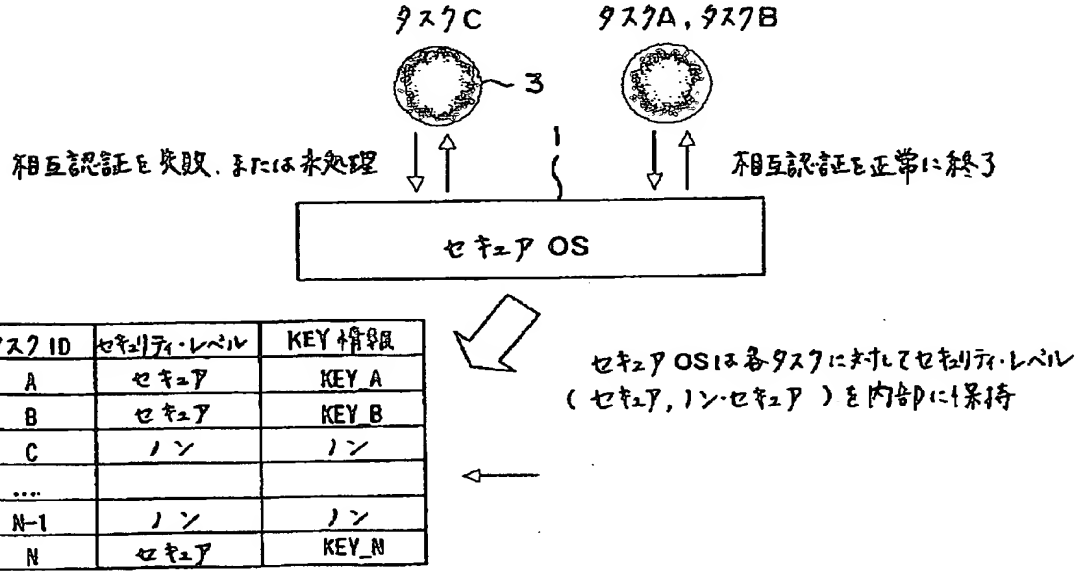
、４，７……テーブル、５……メモリ・ブロック、５ａ……セキュア・メモリ・ブロック、５ｂ……ノン・セキュア・メモリ・ブロック、６……ＳＭＭＵ（メモ管理機構）、８，９……バッファ、１０ａ，１０ｂ……セキュア・メモリ・プール、１１ａ……ノン・セキュア・メモリ・キュー・リスト、１１ｂ……セキュア・メモリ・キュー・リスト、１２……管理情報、１２ａ……メイル・サイズ、１２ｂ……ポインタ。

【書類名】　　図面

【図１】



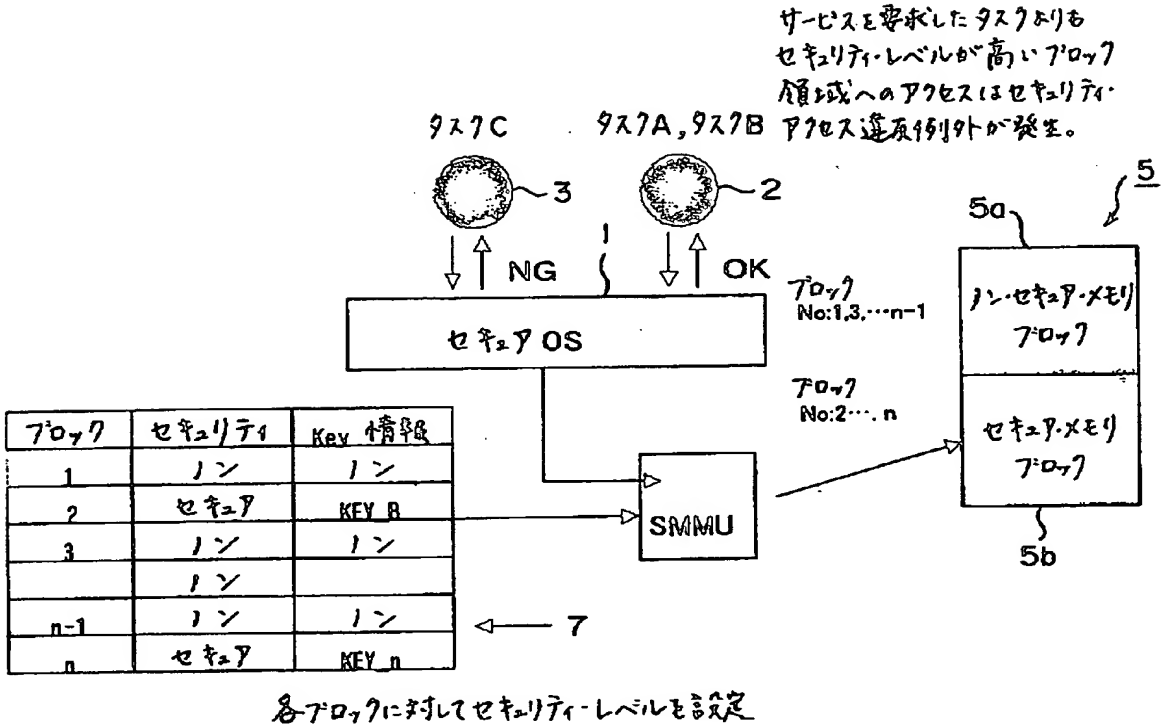
【図２】



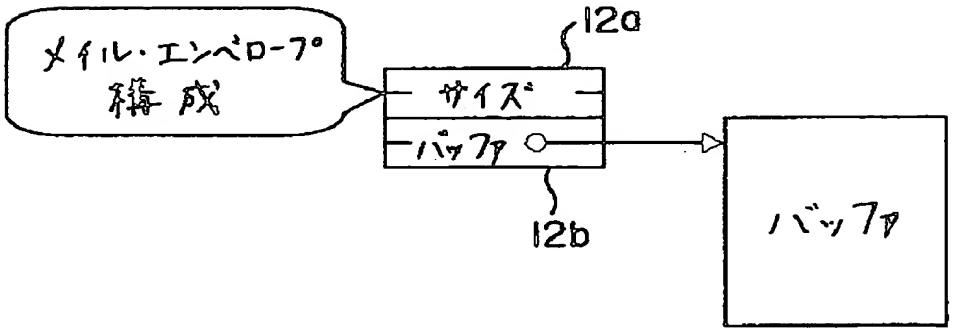
タスクID	セキュリティ・レベル	KEY情報
A	セキュア	KEY_A
B	セキュア	KEY_B
C	ノン	ノン
....		
N-1	ノン	ノン
N	セキュア	KEY_N

セキュアOSは各タスクに対してセキュリティ・レベル（セキュア，ノン・セキュア）を内部に保持

【図３】

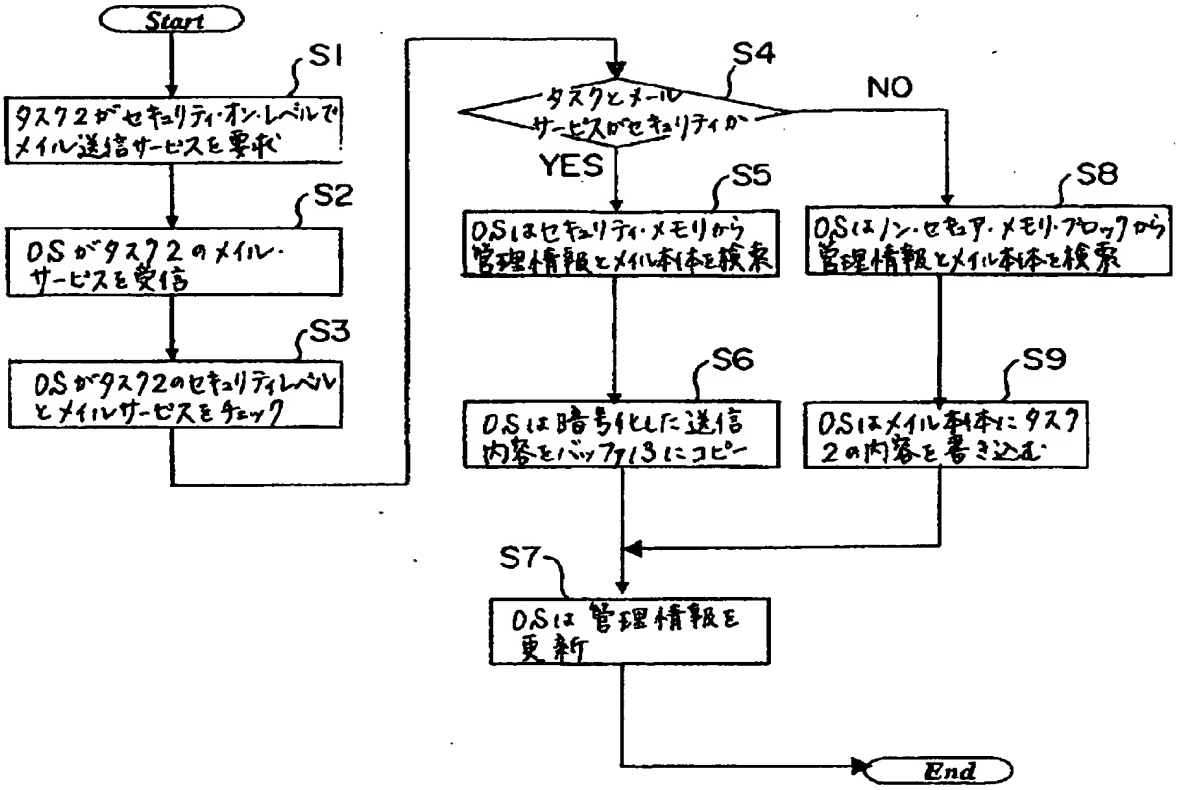


【図４】

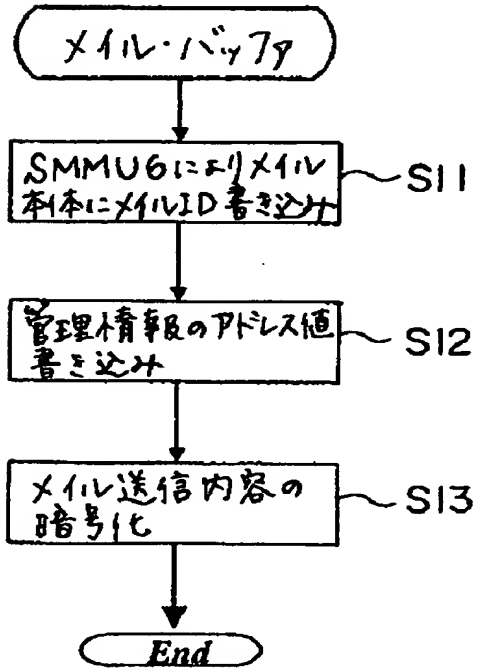


出証特２００１－３０４４７５５

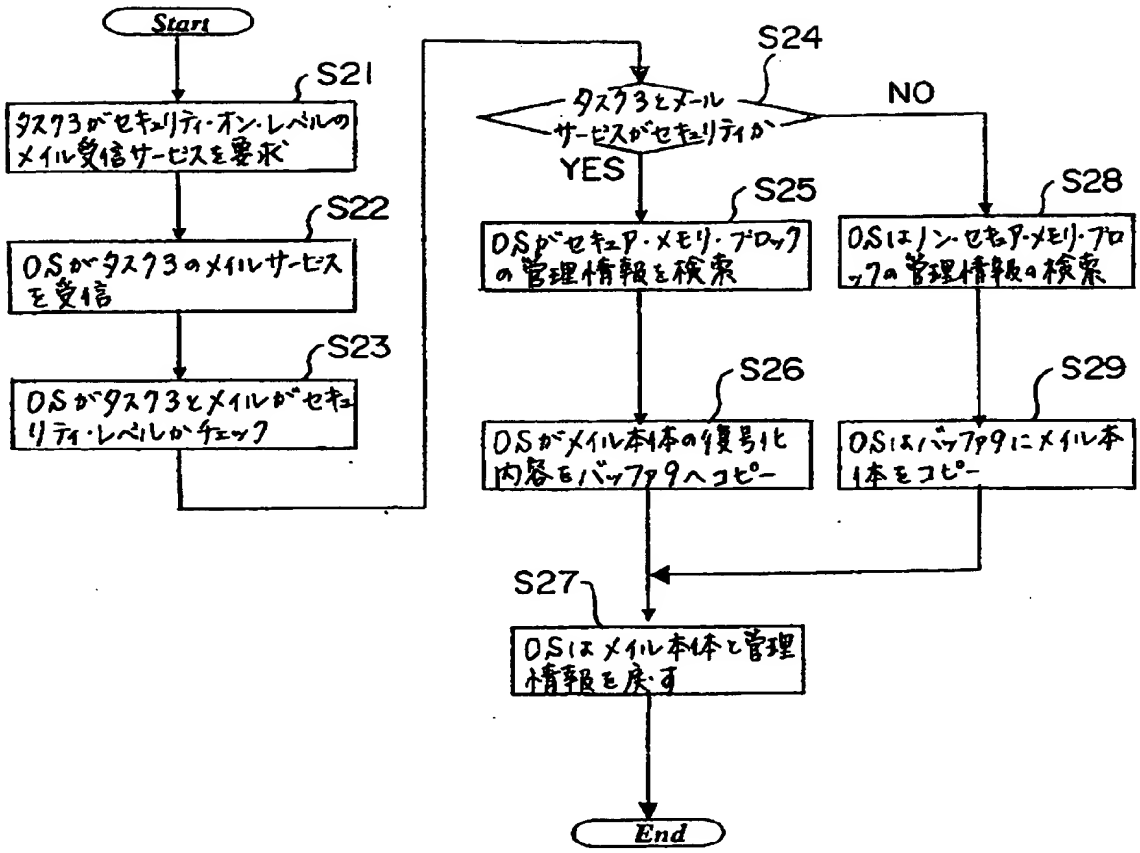
【図５】


Start
S1
タスク2がセキュリティ・オン・レベルでメイル送信サービスを要求
S2
OSがタスク2のメイル・サービスを受信
S3
OSがタスク2のセキュリティレベルとメイルサービスをチェック
S4
タスクとメールサービスがセキュリティか
NO
YES
S5
OSはセキュリティ・メモリから管理情報とメイル本体を検索
S8
OSはノン・セキュア・メモリ・ブロックから管理情報とメイル本体を検索
S6
OSは暗号化した送信内容をバッファ13にコピー
S9
OSはメイル本体にタスク2の内容を書き込む
S7
OSは管理情報を更新
End

【図６】


メイル・バッファ
SMMU6によりメイル本体にメイルID書き込み
S11
管理情報のアドレス値書き込み
S12
メイル送信内容の暗号化
S13
End

【図７】



【図８】

メイル送信

(a) SendMail(int MailBoxNumber, MailBuf *buf, int SecurityLevel)

メイル受信

(b) RecvMail(int MailBoxNumber, MailBuf *buf, int SecurityLevel)

【書類名】　　要約書

【要約】

【課題】　セキュリティを持つタスク間通信の秘匿性を高めるＯＳ上のセキュアなタスク間通信方法を提供すること。

【解決手段】　メイル送信用タスク２側でメイルＩＤ、メイル本体へのアドレスを指定し、セキュアＯＳ１で、メイル送信用タスク２のセキュリティ・レベルと送信用関数のセキュリティ・レベルを基に、セキュア・メモリ・キュー・リスト１１ｂ中の１要素に管理情報を書き込み、メイル送信内容をメイルＩＤ、管理情報のアドレス値、メイル本体のアドレス値を鍵として暗号化した内容をバッファ８に書き込む。

セキュアＯＳ１はメイル受信用タスク３のセキュリティ・レベルと受信用関数のセキュリティ・レベルを基に受信内容の存在するバッファの内容をメイルＩＤ、管理情報のアドレス値、メイル本体のアドレス値を鍵として復号化してメイル受信用タスク３上のバッファ９にコピーする。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社